Job 2

Un **réseau** est un ensemble interconnecté d'éléments, d'entités ou de points, conçu pour permettre **la communication**, **le partage de ressources, ou la distribution d'informations**.

Un **réseau informatique** sert à **connecter** et à **interconnecter** divers dispositifs informatiques.
Tout ceci permet de **faciliter la communication et le partage** de ressources et l'accès à l'information.

Afin de construire un réseau, on a besoin de divers composants tels que :

- **Ordinateurs et périphériques** : Ce sont les appareils qui se connectent au réseau pour accéder aux ressources partagées, communiquer et utiliser les services du réseau.

- **Routeurs** : Les routeurs sont des dispositifs essentiels pour la communication entre les réseaux. Ils déterminent la meilleure voie pour acheminer les données d'un réseau à un autre. Les routeurs sont également souvent équipés de pare-feu pour la sécurité et de capacités de gestion de la bande passante.

- **Commutateurs (Switches)** : Les commutateurs sont des dispositifs qui relient plusieurs appareils au sein d'un réseau local (LAN). Ils fonctionnent au niveau de la couche 2 (liaison de données) du modèle OSI et permettent de transférer les données uniquement aux destinataires appropriés.

- **Serveurs** : Les serveurs sont des ordinateurs conçus pour fournir des services, tels que le stockage de fichiers, la gestion des e-mails, l'hébergement de sites web, la base de données, etc., aux autres appareils du réseau.

- **Modems** : Les modems sont utilisés pour établir la connexion entre le réseau local et Internet, généralement par le biais de technologies telles que DSL, câble ou fibre optique.

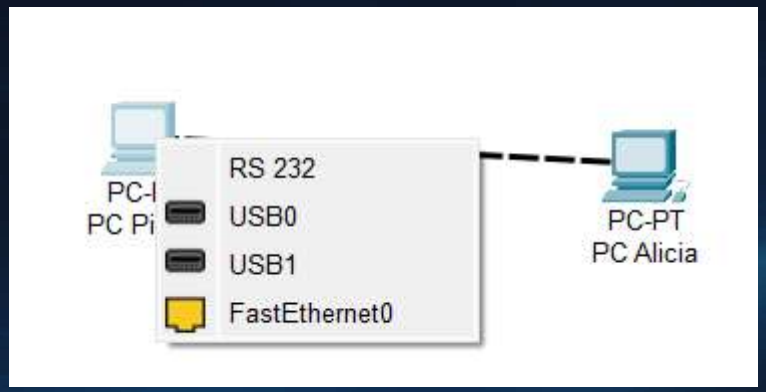
- **Serveurs de stockage en réseau (NAS)** : Les NAS sont des serveurs dédiés au stockage de données. Ils permettent le stockage centralisé de fichiers, ce qui facilite la sauvegarde, le partage et l'accès aux données.
- **Firewalls** : Les pare-feu sont des dispositifs de sécurité qui filtrent le trafic entrant et sortant pour protéger le réseau contre les menaces et les intrusions non autorisées.

- **Onduleurs (UPS)** : Les onduleurs fournissent une alimentation électrique de secours pour garantir le fonctionnement continu du réseau en cas de panne de courant.

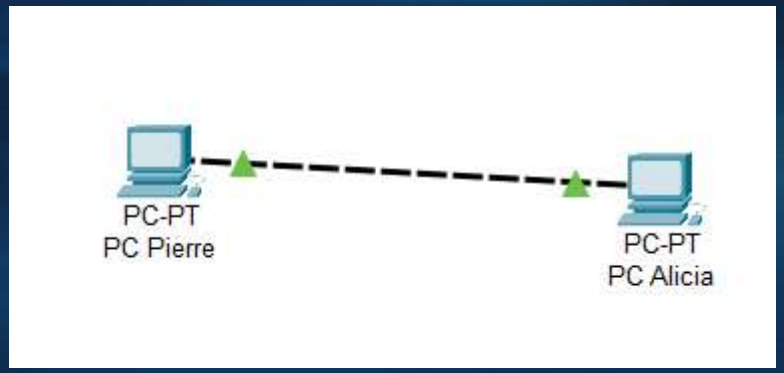
- **Câbles et connecteurs** : Les câbles Ethernet (généralement des câbles RJ-45) sont utilisés pour connecter les appareils au réseau, tandis que les connecteurs, les prises murales et les panneaux de brassage facilitent la connexion des câbles aux appareils et aux commutateurs.

Job 3

Pour relier mes 2 ordinateurs j'ai utilisé un cable copper cross over, il est utilisé pour connecter des dispositifs de même type, tels que deux ordinateurs entre eux.



Voici mes 2 ordinateurs relié



Job 4

Une **adresse IP** est une sorte de **carte d'identité numérique** unique attribuée à chaque appareil connecté à un réseau informatique qui utilise le protocole Internet.
Cette adresse est utilisée pour **identifier et localiser** de manière unique chaque appareil au sein du réseau. Une adresse IP est essentielle pour le routage des données sur le réseau, car elle indique où envoyer les informations.

Les adresses IP ont donc **deux fonctions principales :**

- Identification du pc sur le réseau
- Localisation de l'emplacement géographique de l'appareil

Il existe **deux principales versions d'adresses IP** : **IPv4** et **IPv6**

➢ **IPv4** : est la version d'adresse IP la plus couramment utilisée. Une adresse IPv4 est composée de quatre groupes de chiffres décimaux séparés par des points (par exemple, 192.168.1.1). Chaque groupe de chiffres peut varier de 0 à 255. Cela signifie qu'il y a un nombre limité d'adresses IPv4 disponibles.

- **IPv6** : Pour faire face à la pénurie d'adresses IPv4, IPv6 a été développé. Une adresse IPv6 est beaucoup plus longue et complexe, composée de huit groupes de caractères alphanumériques, séparés par des deux-points (par exemple, 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Cela offre un nombre astronomique d'adresses IP, ce qui garantit qu'il y en aura suffisamment pour prendre en charge la croissance continue d'Internet.

Une **adresse MAC** est une **adresse unique** attribuée à chaque carte réseau ou interface réseau d'un appareil ou d'un composant matériel connecté à un réseau.

Contrairement à une **adresse IP qui peut changer** ou être attribuée dynamiquement, une **adresse MAC est fixe** et **spécifique** à un dispositif réseau. Elle est stockée dans le matériel même de la carte réseau, comme une puce ou une mémoire EEPROM.

Les adresses MAC ne sont généralement **pas visibles sur Internet** et sont **spécifiques à chaque interface réseau d'un appareil**. Elles sont utilisées principalement pour le **contrôle d'accès** et le **routage de données** sur le réseau local.

Une **adresse IP publique** est une adresse qui est **visible** et **accessible depuis l'Internet**. Elle est utilisée pour **identifier un appareil ou un réseau sur Internet**. Les adresses IP publiques sont attribuées par les fournisseurs de services Internet (FSI) et sont généralement **uniques à l'échelle mondiale**, ce qui signifie qu'aucune autre adresse IP publique identique ne devrait exister sur Internet.

Une **adresse IP privée** est utilisée à **l'intérieur d'un réseau local** (LAN) ou d'une organisation pour **identifier des appareils au sein du réseau**. Contrairement aux adresses IP publiques, les adresses IP privées ne sont **pas directement accessibles depuis Internet**. Elles sont destinées à être utilisées **uniquement à l'intérieur du réseau local.**

La **différence entre les deux** est qu'une adresse **IP publique est utilisée pour identifier un appareil sur Internet** tandis qu'une adresse **IP privée est utilisée pour identifier un appareil à l'intérieur d'un réseau local.** Les adresses IP privées sont souvent utilisées pour la sécurité et la gestion du trafic dans un réseau local.

Pour **déterminer l'adresse d'un réseau spécifique** on peut utiliser des calculs de sous-réseau en fonction de **l'adresse IP**, **du masque de sous-réseau** et de la **classe d'adressage appropriés**

- **Classe d'adressage** : La classe d'adressage (A, B, C, D, ou E) est déterminée en fonction de la taille du réseau. Par exemple, les adresses de classe A sont généralement utilisées pour les réseaux très vastes, tandis que les adresses de classe C sont utilisées pour des réseaux plus petits.

- **Masque de sous-réseau** : Le masque de sous-réseau détermine la taille du réseau et la partie de l'adresse IP qui identifie le réseau. Il est généralement spécifié en notation CIDR (Classless Inter-Domain Routing) et indique le nombre de bits dans la partie réseau de l'adresse IP.

- **Adresse IP** : Vous avez besoin d'une adresse IP spécifique pour déterminer l'adresse du réseau. Cette adresse IP doit faire partie du réseau dont vous souhaitez trouver l'adresse.

- **Localisation dans la topologie réseau** : La place du réseau dans la hiérarchie d'un réseau plus vaste est également importante. Par exemple, un réseau local (LAN) peut être relié à un réseau plus large, et cela influe sur la définition de son adresse.

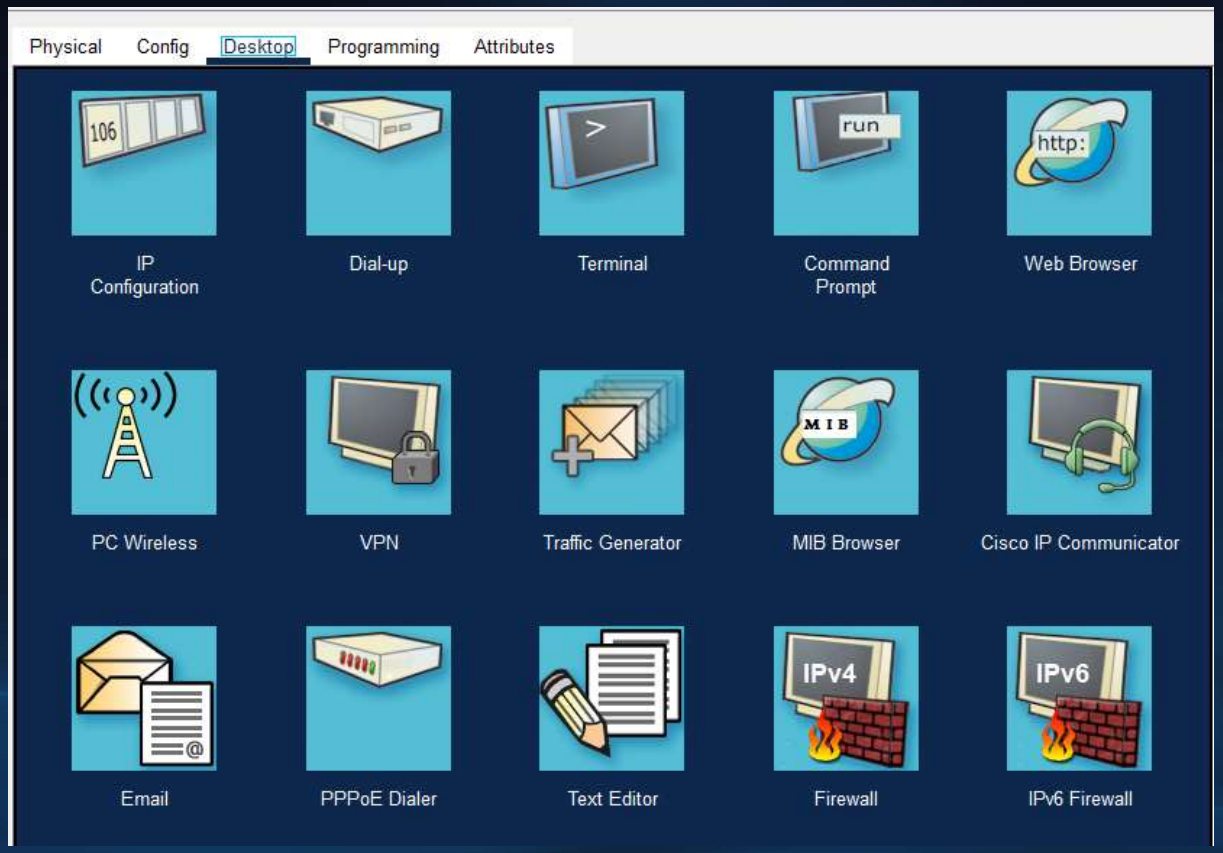
Si l'adresse IP est "192.168.1.1" et le masque de sous-réseau est "255.255.255.0", **l'adresse réseau sera** "192.168.1.0"

Job 5

Pour vérifier que les IP des pc de pierre et d'Alicia sont correct, il faut :

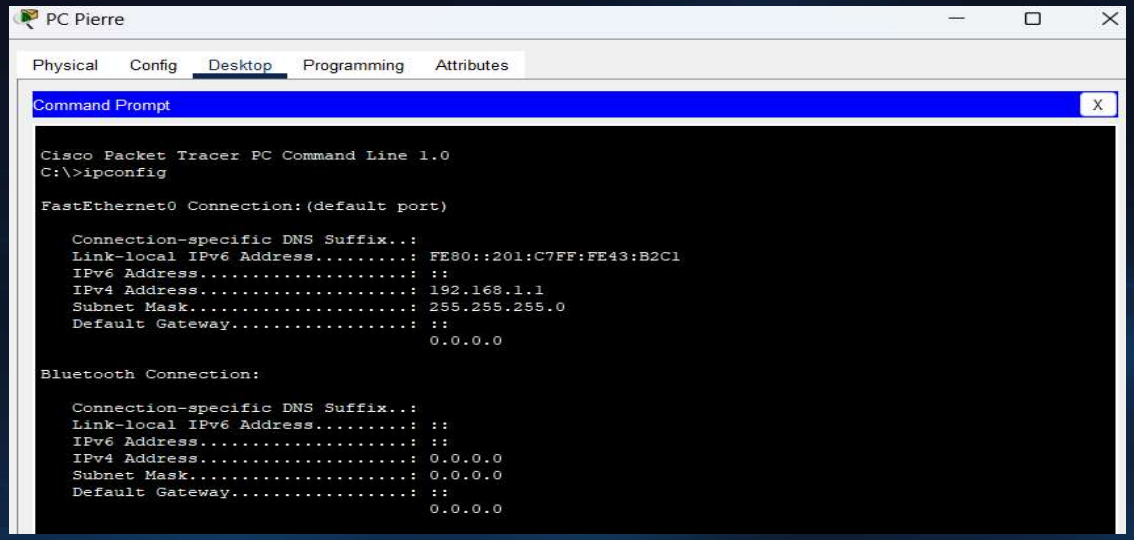
- cliquer sur le PC correspondant

- aller sur l'onglet "Desktop"

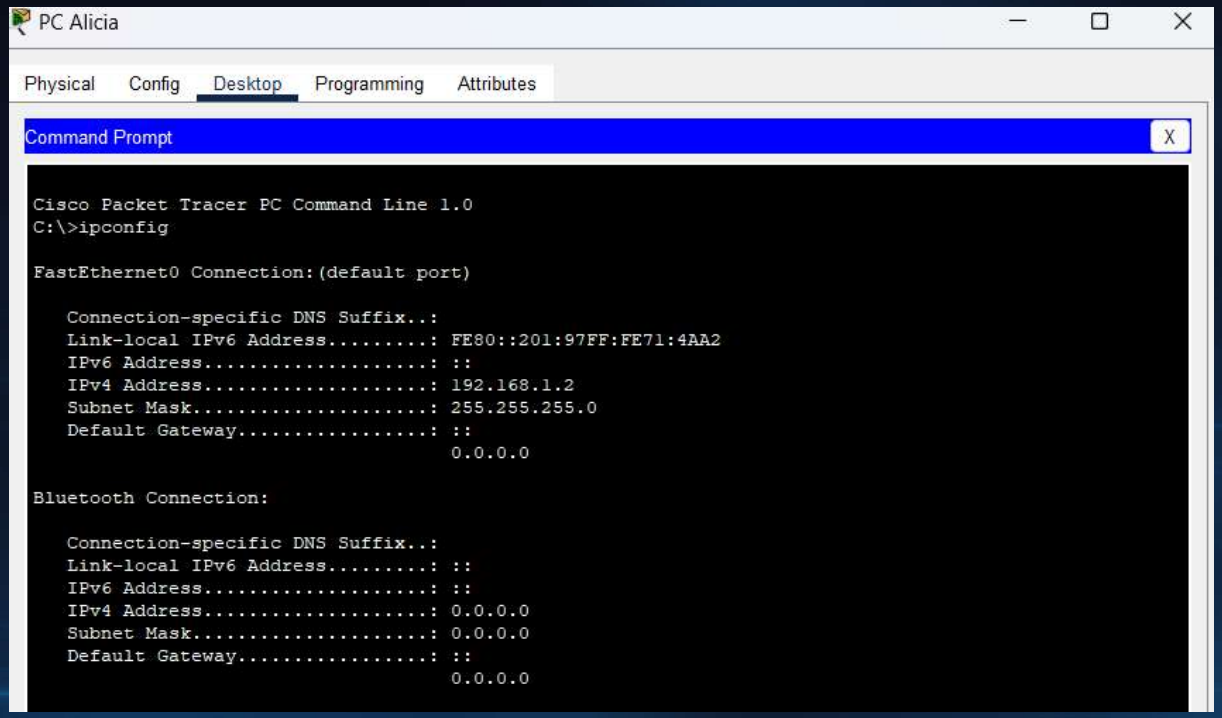


- ouvrir " command prompt "
- tapper la ligne de commande *"ipconfig"*

Ip pc de Pierre



IP pc de Alicia



Job 6

Afin de savoir si la **connectivité entre les 2 pc est bonne**, j'effectue un ping depuis le pc de pierre vers l'ip d'Alicia.

Depuis le **PC de Pierre**, dans le terminal, je tape la **commande** *"ping adresse_ip _de_la_machine_cible"*

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Depuis le **PC d'Alicia**

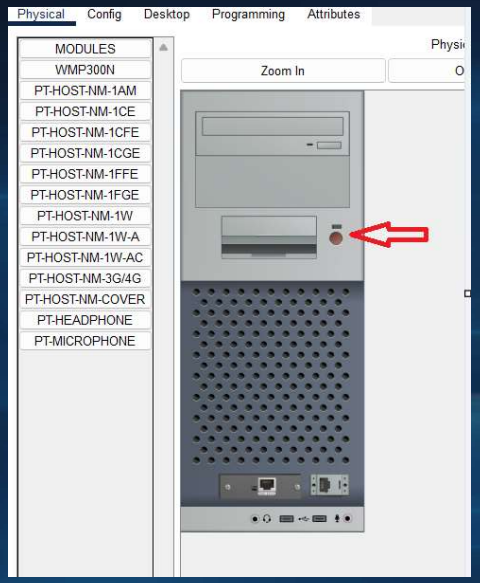
```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

On peut voir que la connectivité entre les 2 pc est bonne.

Job 7

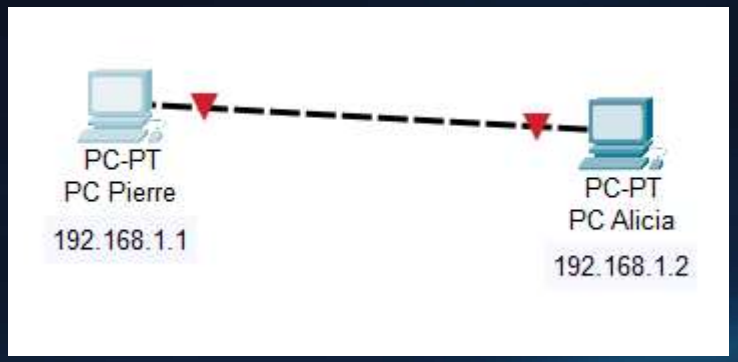
Pour éteindre le pc de pierre il faut :

- cliquer sur celui-ci
- Appuyer sur le bouton d'alimentation afin de l'éteindre



(le voyant lumineux s'éteint)

Une fois effectué lorsqu'on revient sur notre schéma, on devrait se rendre compte que le cable reliant nos 2 pc a changé voir ci dessous



Depuis le **terminal d'Alicia** lorsqu'on effectue à nouveau un ping **vers le PC de Pierre,** on remarque que celui-ci **ne reçoit pas les paquets envoyé** depuis le PC d'Alicia

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

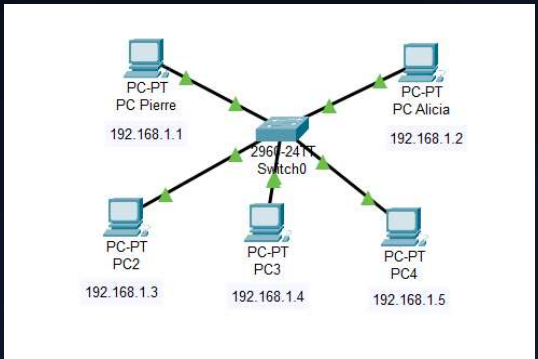
Lorsqu'on éteint un ordinateur, le système d'exploitation s'arrête, mais aussi le matériel associé, y compris la carte réseau. **L'interface réseau** de l'ordinateur est **déconnectée du réseau** et ne peut **plus recevoir ni traiter de paquets.**

Lorsqu'un ordinateur **émet des paquets vers un autre**, il utilise généralement une **résolution ARP** pour trouver l'adresse MAC de la cible. Lorsque la cible est éteinte, il n'y a pas de réponse à cette requête ARP, et les paquets ne peuvent pas être correctement acheminés.

En l'absence d'une réponse ARP de la cible, les paquets émis par un autre ordinateur vers cette cible éteinte **ne sont pas livrés**. Le protocole de transport sous-jacent (généralement TCP ou UDP) gérera les retransmissions en cas de non-réponse, mais ces tentatives restent sans succès tant que la cible restera éteinte.

Job 8

Afin de mettre 5 ordinateurs sur le même réseau on va utiliser **un switch**



On ajoute ensuite une adresse IP **à chacun de nos nouveaux PC** tout comme pour le PC de Pierre et d'Alicia.

Puis ensuite de la même façon que pour le **JOB 6**, on réalise des ping entre nos différents PC afin de vérifier qu'ils soient bien tous connectés sur le même réseau.

Sous linux on aurait pu avec **une seule commande** ping tout les pc
La commande est *" for ip in 192.168.1.1 192.168.1.2 192.168.1.3 192.168.1.4; do ping -c 4 $ip; done "*

Cisco Packet Tracer ne permet pas de faire avec une seule commande, il faut donc tester **chaque pc un à un**.

Un switch est dispositifs couramment utilisés dans les réseaux locaux (LAN) pour connecter plusieurs appareils au sein d'un réseau, ses caractéristiques sont :

- **Fonctionnement intelligent** : Un switch est un dispositif intelligent qui fonctionne au niveau de la couche 2 (liaison de données) du modèle OSI. Il examine les adresses MAC des paquets pour déterminer à quel port envoyer le trafic, ce qui permet un transfert de données plus efficace et sélectif.

- **Acheminement intelligent** : Un switch a la capacité de déterminer quel port est connecté à quel appareil, ce qui signifie que les paquets sont transmis uniquement aux ports concernés, minimisant ainsi le trafic réseau inutile.

- **Haute performance** : Les switches offrent des performances élevées et conviennent aux réseaux où la bande passante est essentielle. Ils sont capables de traiter de grandes quantités de trafic simultanément.

- **Sécurité accrue** : Les switches offrent une certaine sécurité car ils isolent le trafic entre les ports, limitant la visibilité des paquets à d'autres appareils du réseau.

Quand au HUB ses caractéristiques sont :

- **Fonctionnement passif** : Un hub est un dispositif passif qui fonctionne au niveau de la couche 1 (physique) du modèle OSI. Il se contente de diffuser les paquets reçus à tous les ports, sans distinction.

- **Diffusion de paquets** : Tous les paquets entrants sont répétés sur tous les ports du hub, ce qui peut entraîner une utilisation inefficace de la bande passante et des collisions sur le réseau.

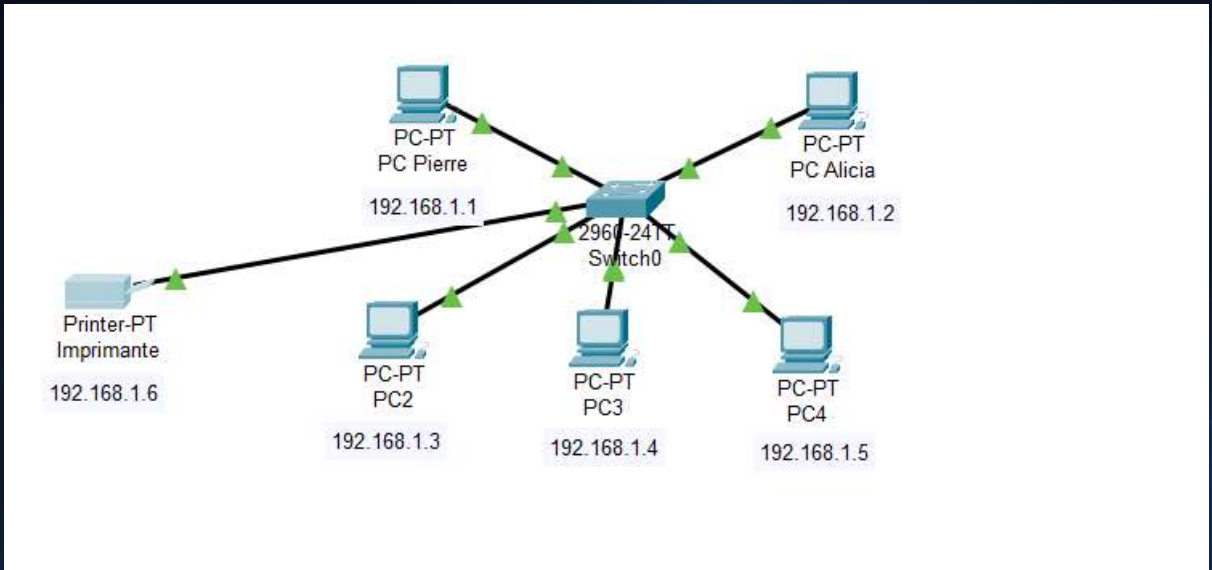
- **Performances plus faibles** : Les hubs sont moins efficaces que les switches, en particulier dans les réseaux comportant un trafic important. Les collisions et les conflits de données sont plus courants.

- **Moins sécurisé** : En raison de la diffusion de paquets à tous les ports, les hubs offrent moins d'isolation et de sécurité. Tous les appareils du réseau peuvent potentiellement voir le trafic de chaque autre appareil.

Les avantages du switch sont qu'il est plus **performant**, **plus efficace**, et il offre une **meilleure sécurité** par rapport à un hub. Pour la plupart des réseaux modernes, l'utilisation d'un switch est préférable en raison de sa capacité à gérer le trafic de manière **plus intelligente et à minimiser les collisions**. **Les hubs** sont moins courants aujourd'hui, sauf dans des cas très spécifiques où la **simplicité et le coût sont des priorités**.

Job 9

Schéma du réseau



Sur mon réseau on peut voir **5 ordinateurs** ainsi qu'une **imprimante reliée sur un switch.**

Chaque périphérique dispose d'une adresse ip qui lui est propre.

Il y a **plusieurs avantage au fait de réaliser un schéma de réseau** notamment au niveau de :

- **La visualisation et la compréhension**, permet une représentation visuelle claire de la topologie et de la configuration du réseau.

  Cela facilite la compréhension de la manière dont les dispositifs réseau sont connectés et interagissent.

- **Sécurité réseau** : La visualisation du réseau aide à identifier les vulnérabilités potentielles et à planifier des mesures de sécurité pour protéger le réseau.

- **Dépannage et résolution des problèmes** : Lorsqu'un problème réseau se produit, un schéma réseau peut être un outil précieux pour identifier rapidement la source du problème. Il permet de suivre la trajectoire du trafic, les connexions et les configurations.

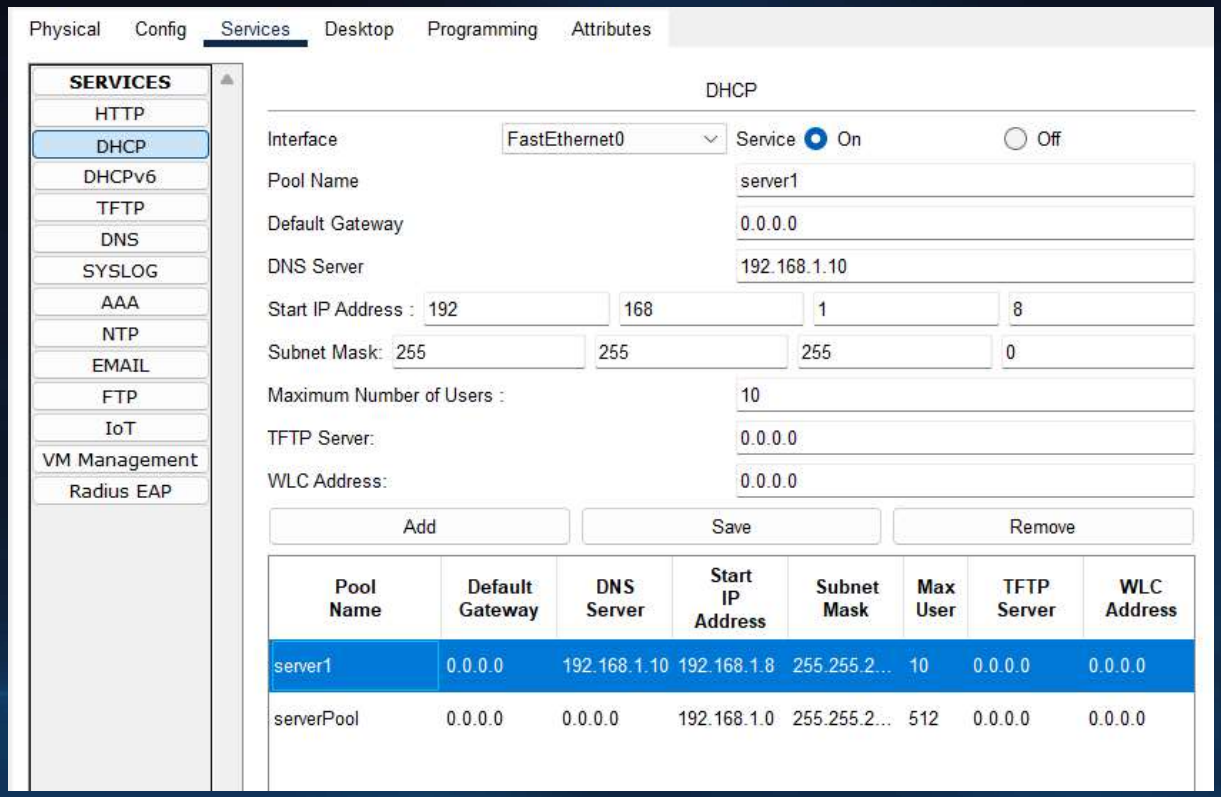
- **Planification réseau :** Les schémas réseau sont essentiels pour la planification et la conception de réseaux. Ils aident à déterminer l'emplacement des dispositifs, des serveurs, des commutateurs, des routeurs, etc., pour une mise en œuvre optimale.

Job 10

Pour mettre en place un **serveur DHCP** :

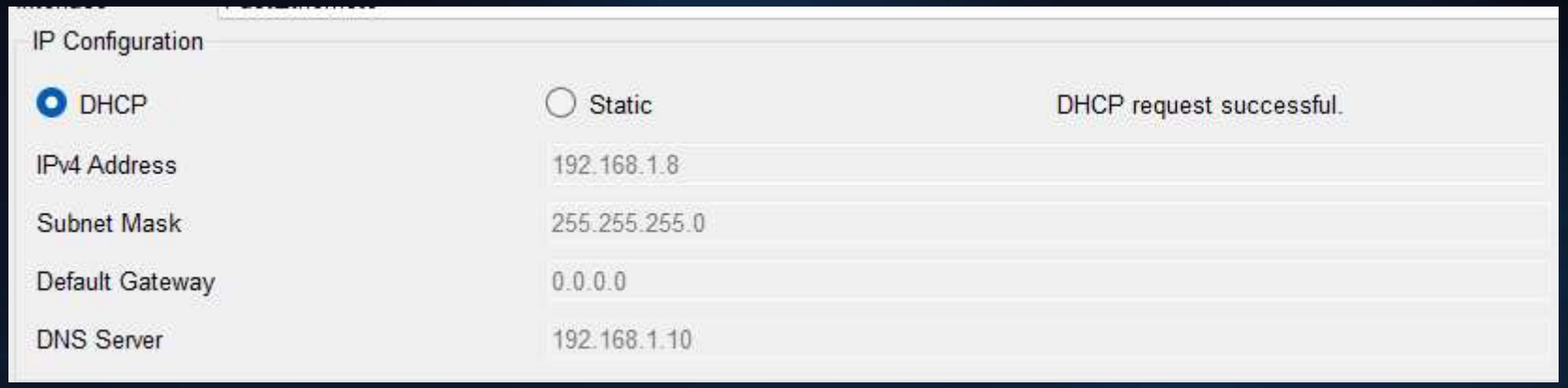
- je connecte mon serveur à mon switch

- je clique ensuite sur mon serveur puis dans l'onglet service je vais sur DHCP



➢ On configure ensuite le serveur en activant le service " on ", ensuite on entre le nom du serveur, ainsi que son adresse ip qu'on aura préalablement entrée puis le nombre maximum d'users sur le réseau.

➢ Il ne reste plus qu'à connecter les ip des ordinateurs en DHCP



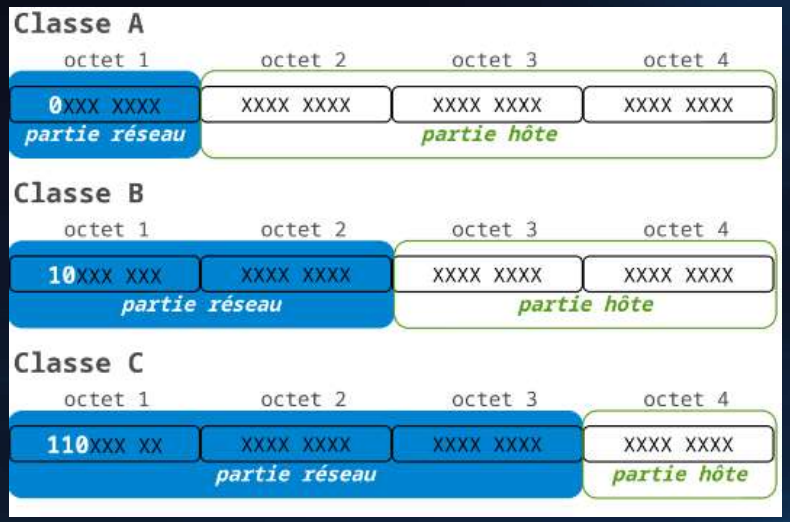
L'adresse IP statique est attribuée **manuellement et ne change pas.**

L'adresse IP attribuée par DHCP est **automatiquement gérée par un serveur DHCP** et peut **varier à chaque connexion**. Le choix entre ces deux méthodes dépend des besoins spécifiques de votre réseau et de la flexibilité requise pour gérer les adresses IP.

Job 11

	adresse reseau	pool adresse ip	adresse broadcast	Masque sous réseaux	nbr hôtes
1 sous réseau 12 hôtes	10.0.0.0	10.0.0.1 à 10.0.0.14	10.0.0.15	255.255.255.240	2^4 - 2 (adresse reseau + adresse broadcast) = 14 hôtes
1 er sous réseaux 30 hôtes	10.0.0.16	10.0.0.17 à 10.0.0.46	10.0.0.47	255.255.255.224	
2 eme sous réseaux 30 hôtes	10.0.0.48	10.0.0.49 à 10.0.0.78	10.0.0.79		
3 eme sous réseaux 30 hôtes	10.0.0.80	10.0.0.81 à 10.0.0.110	10.0.0.111		2^5 - 2 (adresse reseau + adresse broadcast) = 30 hôtes
4 eme sous réseaux 30 hôtes	10.0.0.112	10.0.0.113 à 10.0.0.142	10.0.0.143		
5 eme sous réseaux 30 hôtes	10.0.0.144	10.0.0.145 à 10.0.0.174	10.0.0.175		
1 er sous réseaux 30 hôtes	10.0.0.176	10.0.0.177 à 10.0.1.46	10.0.1.47	255.255.255.128	
2 eme sous réseaux 30 hôtes	10.0.1.48	10.0.1.49 à 10.0.1.174	10.0.1.175		
3 eme sous réseaux 30 hôtes	10.0.1.176	10.0.1.177 à 10.0.2.46	10.0.2.47		2^7 - 2 (adresse reseau + adresse broadcast) = 126 hôtes
4 eme sous réseaux 30 hôtes	10.0.2.48	10.0.2.49 à 10.0.2.174	10.0.2.175		
5 eme sous réseaux 30 hôtes	10.0.2.176	10.0.2.177 à 10.0.3.46	10.0.3.47		
1 er sous réseaux 30 hôtes	10.0.3.48	10.0.3.49 à 10.0.4.46	10.0.4.47	255.255.255.1	
2 eme sous réseaux 30 hôtes	10.0.4.48	10.0.4.49 à 10.0.5.46	10.0.5.47		
3 eme sous réseaux 30 hôtes	10.0.5.48	10.0.5.49 à 10.0.6.46	10.0.6.47		2^8 - 2 (adresse reseau + adresse broadcast) = 254 hôtes
4 eme sous réseaux 30 hôtes	10.0.6.48	10.0.6.49 à 10.0.7.46	10.0.7.47		
5 eme sous réseaux 30 hôtes	10.0.7.48	10.0.7.49 à 10.0.8.46	10.0.8.47		

On a utilisé une adresse de **classe A** car celle-ci permet d'avoir un grand nombre **un très grand nombre d'hôtes** , en effet celle-ci alloue 8 seulement 8 bit aux sous réseaux et 24 bit à la partie hôte.



En fonction de nos besoin de terme **de nombres de sous réseaux** ou **d'hôtes** on choisira un réseau de classe **A, B** ou **C**.

Un réseau de **classe A** offre **beaucoup d'hôtes possibles** mais **peu de sous réseaux**, celui de **classe B** est un compromis entre les deux et celui de **type C** offre une **grande partie réseau** mais **peu d'hôtes.**

Job 12

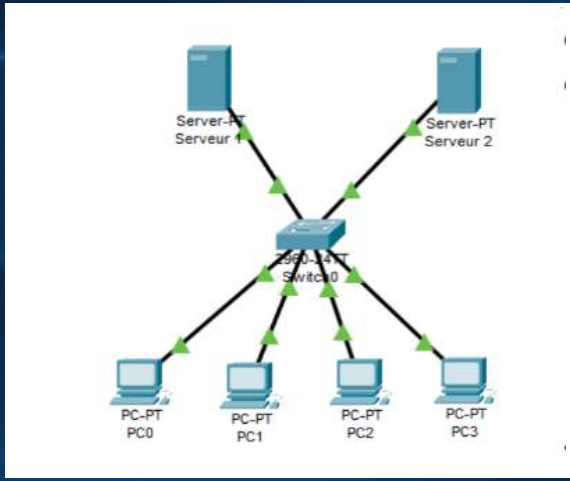
Couche OSI	Description des rôles	Matériels/Protocoles/Technologies associés

Couche 7 - Application	Donne une interface pour les utilisateurs et les applications pour accéder au réseau. Gère les protocoles de communication applicative.	HTML, FTP, SSL/TLS
Couche 6 - Présentation	Gère la traduction, la compression et le chiffrement des données. Assure la conversion des données dans un format compréhensible par les applications.	SSL/TLS
Couche 5 - Session	Établit, gère et termine les sessions de communication entre les applications. Gère la synchronisation et la reprise après panne.	PPTP , SSL/TLS

Couche 4 - Transport	Contrôle de bout en bout de la communication. Garantit la transmission correcte des données.	TCP, UDP
Couche 3 - Réseau	connectivité entre les nœuds du réseau. Choisis le meilleur chemin pour acheminer les données et gère les adresses logiques.	IPv4, IPv6, routeur
Couche 2 - Liaison de données	transmission des données à travers un lien physique. Gère la détection et la correction d'erreurs.	Ethernet, MAC, câble RJ45, Wi-Fi

Couche 1 - Physique	Câbles, signaux électriques et optiques, les connecteurs.	Fibre optique11

Job 13



L'architecture de ce réseau est **un réseau en étoile**, tous les périphériques **sont connectés à un concentrateur central** ou à un **commutateur**. **Chaque périphérique** a une connexion dédiée au **concentrateur ou au commutateur**, ce qui signifie qu'ils ne sont **pas directement connectés les uns aux autres.**
Elle est couramment utilisée dans de nombreuses situations car cette topologie présente **plusieurs avantages** :

- **Facilité de gestion :** Un réseau en étoile est relativement simple à configurer et à gérer. En cas de panne ou de besoin de maintenance, il est plus facile d'isoler et de diagnostiquer les problèmes, car chaque connexion est indépendante.

- **Fiabilité** : En cas de panne d'un câble ou d'un périphérique, seuls le périphérique affecté et la connexion vers le concentrateur ou le commutateur sont touchés. Les autres périphériques restent opérationnels. Cela augmente la fiabilité globale du réseau.

- **Sécurité** : En raison de la nature centralisée de la topologie, il est plus facile de mettre en place des mesures de sécurité, comme la surveillance du trafic, la gestion des autorisations d'accès et le pare-feu.

- **Isolation des problèmes** : Si un périphérique présente des problèmes ou génère du trafic anormal, cela n'affectera généralement pas les autres périphériques du réseau. Cela aide à isoler les problèmes plus rapidement.

Néanmoins, il y a aussi des **inconvénients** notamment dû au fait qu'un réseau en étoile **dépend fortement de la fiabilité du concentrateur ou du commutateur central**. Si ce dernier **tombe en panne**, tout le réseau peut être affecté. De plus, cette topologie nécessite généralement plus de câblage que certaines autres topologies

L'adresse Ip de ce réseau est 192.168.10.0 et son **adresse de diffusion** est 192.168.10.255

L'adresse de diffusion permet notamment d'envoyer des données à tous les périphériques du réseau.

Si on part du principe qu'on ne dispose que d'un **switch comme indiqué sur le schéma, et** vu qu'un switch **ne dispose que de 24 slots** on ne pourra brancher que **24 machines** au maximum sur ce réseau.

Si on avait **un plus grand nombre de switch**, on pourrait monter jusqu'à **254 machines** sur ce réseau.

Job 14

Chaque chiffre de l'adresse ip se décompose dans un bloc linaire de 8 bits.

Chaque bit successif à gauche représente le **double de la valeur,** soit : 128 64 32 16 8 4 2 1

La valeur de chaque chiffre d'un nombre binaire est déterminée par sa **position** dans le tableau.

La somme de toutes ces valeurs de colonne pour **chaque chiffre** donne la représentation décimale du nombre binaire.

En utilisant cette logique, nous pouvons facilement calculer la représentation décimale d'un nombre binaire comme 11100011 par exemple. Il nous suffit d'activer les bits respectifs et de calculer la valeur des valeurs décimales.

8e bit (128)	7e bit (64)	6e bit (32)	5e bit (16)	4e bit (8)	3e bit (4)	2e bit (2)	1e bit (1)
1	1	1	0	0	1	1	1

11100011 revient à **additionner** 126 + 64 + 32 + 2 + 1 ce qui fait **231.**

Si on décompose l'id **145.32.59.24** en prenant chaque bloc séparément, nous avons :

145 qui est égal à **128 + 16 + 1** ce qui donne donc en binaire **10010001**

32 qui est égal à **32** ce qui donne donc en binaire **00100000**

59 qui est égal à **32+16+8+2+1** ce qui donne donc en binaire **00111011**

24 qui est égal à **16+8** ce qui donne donc en binaire **00011000**

Le binaire de l'adresse ip **145.32.59.24** est donc **10010001.00100000.00111011.00011000**
Le binaire de l'adresse ip **200.42.129.16** est donc **11001000.00101010.10000001.00010000**
Le binaire de l'adresse ip **14.82.19.54** est donc **00001110.01010010.00010011.00110110**

Job 15

Le **routage** consiste à déterminer le **meilleur chemin ou l'itinéraire** pour faire parvenir **les données d'une source à une destination**. Le routage est essentiel pour **permettre la communication efficace** entre différents réseaux, sous-réseaux et hôtes (périphériques) au sein d'un réseau.
Il permet d'assurer que les données sont acheminées de manière efficace en prenant en compte **les contraintes de performances, de disponibilité et de coût.**

Un **gateway** est un dispositif matériel ou logiciel utilisé **pour connecter deux réseaux informatiques** ayant **des protocoles**, **des formats de données** ou **des architectures différentes**. Les passerelles jouent un rôle essentiel dans la communication entre réseaux hétérogènes, permettant aux données de passer d'un réseau à l'autre de manière transparente.

Un **VPN** est un service ou une technologie qui permet de **créer une connexion sécurisée et chiffrée** entre un dispositif (comme un ordinateur, un smartphone ou une tablette) et un réseau. Les VPN sont largement utilisés pour **améliorer la sécurité**, **la confidentialité** et **l'anonymat** des communications en ligne

Le **DNS** est un système informatique qui permet de **traduire les noms de domaine en adresses IP.**
Le DNS assure **la correspondance** entre les noms de domaine et les adresses IP, ce qui facilite la navigation sur le web et l'accès aux ressources en ligne.